65B/XXX/NP

NEW WORK ITEM PROPOSAL

Proposer	Date of proposal
USA	March 2001
TC/SC	Secretariat
65 B	USA
Date of circulation	Closing date for voting
2001-04-XX	2001-07-XX

A proposal for a new work item within the scope of an existing technical committee or subcommittee shall be submitted to the Central Office. The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information. The proposer may be a National Committee of the IEC, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Committee of Action or one of the advisory committees, or the General Secretary. Guidelines for proposing and justifying a new work item are given in ISO/IEC Directives, Part 1, Annex C (see extract overleaf). **This form is not to be used for amendments or revisions to existing publications.**

The proposal (to be completed by the proposer)

Title of proposal

IEC 61131-X: Programmable controllers – Part X: Functional safety

☒ Standard	☐ Technical Report

Scope (as defined in ISO/IEC Directives, Part 3, 6.2.1)

This international standard establishes the characteristics of a programmable controller required only when it is intended to be used as the logic element of a safety-related system. This standard is based on IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" in which a programmable controller – including its I/O – falls under what's identified as a Type B high complexity subsystem – specifically a logic element - of a safety-related system.

Purpose and justification, including the market relevance and relationship to Safety (Guide 104), EMC (Guide 107), Environmental aspects (Guide 109) and Quality assurance (Guide 102) . (attach a separate page as annex, if necessary)

To provide a product specific standard for programmable controller manufacturers and users to develop and use a programmable controller compatible with IEC 61508 functional safety requirements.

Target date	for first CD June 2002	for IS June 2004
Estimated number of meetings 6	Frequency of meetings 2 per year	Date and place of first meeting: .....
Proposed working methods	☒ E-mail	☐ ftp

Relevant documents to be considered

IEC 61508

Relationship of project to activities of other international bodies

Liaison organizations	**Need for coordination within ISO or IEC**
SC65A	

Preparatory work

Check one of the two following boxes

☒ A draft is attached for vote and comment ☐ An outline is attached

We nominate a project leader as follows in accordance with ISO/IEC Directives, Part 1, 2.3.4 (name, address, fax and e-mail): Dr. Ray Turk - Rockwell Automation - 1 Allen Bradley Drive - Mayfield Heights, OH 44124 USA - Tel: 1-440-646-3999 - Fax: 1-440-646-3993 - E-mail: raturk@ra.rockwell.com

Concerns known patented items (see ISO/IEC Directives, Part 2)	**Name and/or signature of the proposer**
☐ yes ☒ no	
If yes, provide full information as an annex	

Comments and recommendations from the TC/SC officers

Comments with respect to the proposal in general, and recommendations thereon		
1) Work allocation ☐ Project team	☐ New working group	☐ Existing working group no:
2) Draft suitable for direct submission as ☐ CD	☐ CDV	
3) General quality of the draft (conformance with ISO/IEC Directives, Part 3) ☐ Little redrafting needed	☐ Substantial redrafting needed	☐ no draft (outline only)
4) Relationship with other activities In IEC In other organizations		
Other remarks		
Remarks from the TC/SC officers		
Remarks from the Sector Board		

Elements to be clarified when proposing a new work item

Title

Indicate the subject matter of the proposed new standard.

Indicate whether it is intended to prepare a standard, a technical report or an amendment to an existing standard.

Scope

Give a clear indication of the coverage of the proposed new work item and, if necessary for clarity, exclusions.

Indicate whether the subject proposed relates to one or more of the fields of safety, EMC, the environment or quality assurance.

Purpose and justification

Give details based on a critical study of the following elements wherever practicable.

a) The specific aims and reason for the standardization activity, with particular emphasis on the aspects of standardization to be covered, the problems it is expected to solve or the difficulties it is intended to overcome.

b) The main interests that might benefit from or be affected by the activity, such as industry, consumers, trade, governments, distributors.

c) Feasibility of the activity: Are there factors that could hinder the successful establishment or general application of the standard?

d) Timeliness of the standard to be produced: Is the technology reasonably stabilized? If not, how much time is likely to be available before advances in technology may render the proposed standard outdated? Is the proposed standard required as a basis for the future development of the technology in question?

e) Urgency of the activity, considering the needs of the market (industry, consumers, trade, governments etc.) as well as other fields or organizations. Indicate target date and, when a series of standards is proposed, suggest priorities.

f) The benefits to be gained by the implementation of the proposed standard; alternatively, the loss or disadvantage(s) if no standard is established within a reasonable time. Data such as product volume of value of trade should be included and quantified.

g) If the standardization activity is, or is likely to be, the subject of regulations or to require the harmonization of existing regulations, this should be indicated.

If a series of new work items is proposed, the purpose and justification of which is common, a common proposal may be drafted including all elements to be clarified and enumerating the titles and scopes of each individual item.

Relevant documents

List any known relevant documents (such as standards and regulations), regardless of their source. When the proposer considers that an existing well-established document may be acceptable as a standard (with or without amendments), indicate this with appropriate justification and attach a copy to the proposal.

Cooperation and liaison

List relevant organizations or bodies with which cooperation and liaison should exist.

Preparatory work

Indicate the name of the project leader nominated by the proposer.

IEC 61131-X
Programmable controllers – Part X: Functional safety

1 Scope

This international standard establishes the characteristics of a programmable controller required only when it is intended to be used as the logic element of a safety-related system. This standard is based on IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" in which a programmable controller – including its I/O – falls under what's identified as a Type B high complexity subsystem – specifically a logic element - of a safety-related system.

This standard does not include the functional safety requirements of the overall safety-related system – consisting of sensors, a logic element, and actuators - or the functional safety requirements of the ultimate application of the system. The latter is typically expressed as a safety integrity level (SIL) value and should be given in the application standard. This standard does extract the safety lifecycle aspects of IEC 61508 applicable to programmable controllers and applies them to the safety lifecycle of a programmable controller.

Because of the variety of possible safety applications of programmable controllers, this standard only specifies the characteristics of the programmable controller necessary to determine and to comply with the safety integrity of a safety-related system. The results of an evaluation of a programmable controller to this standard are: a Probability of Failure on Demand (PFD) value, a Probability of Failure per Hour (PFH) value, a value for the safe failure fraction (SFF), a diagnostic coverage (DC) value, and a verification that the specified programmable controller manufacturer's safety lifecycle processes are in place. These values can be used by the safety-related system manufacturer to calculate the PFD or PFH of the safety-related system. The PFD or PFH of a safety-related system is just the sum of the PFD or PFH values for the sensors, logic element, and actuators making up the system. The PFD or PFH of the system is directly related to a SIL value that is specified for a particular application of a safety-related system.

This standard can also be used to verify that a programmable controller is fit for use with safety-related systems with specific safety integrity requirements. Safety integrity applies solely to a safety-related system and is a measure of the likelihood of that system to satisfactorily achieve the necessary risk reduction in a safety-related application. Risk is a measure of the frequency and consequence of a hazardous event occurring.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 61508-1: 1998-12, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

65A/294/FDIS (IEC 61508-2), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3: 1998-12, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4: 1998-11, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5: 1998-11, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

65A/295/FDIS (IEC 61508-6), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of Parts 2 and 3*

3 Definitions and abbreviations

architecture
specific configuration of hardware and software elements in a system

channel
element or group of elements that independently perform(s) a function
EXAMPLE – A two channel (or dual-channel) configuration is one with two channels that independently perform the same function
NOTE 1: The elements within a channel could include input/output modules, a logic element (system), sensors, and actuators (final elements).
NOTE 2: The term can be used to describe a complete system, or a portion of a system (for example, sensors or a final element). (taken from IEC 61508-4)

common cause failure
failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure (taken from IEC 61508-4)

dangerous failure
failure which has the potential to put the safety-related system in a hazardous or fail-to-function state (taken from IEC 61508-4)

diagnostic coverage
fractional decrease in the probability of dangerous hardware failure resulting from the operation of the automatic diagnostic tests (taken from IEC 61508-4)

E/E/PE
electrical/electronic/programmable electronic

EUC
equipment under control

Fit for use
based on its characteristics and parametric values, a subsystem does not exceed its assumed share of a system's likelihood of satisfactorily achieving the necessary risk reduction

fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors (taken from IEC 61508-4)

functional safety
part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related system, other technology safety-related systems and external risk reduction facilities (taken from IEC 61508-4)

Note: Functional safety is, in essence, the ability of a safety-related system to carry out the actions necessary to maintain a safe state.

high complexity safety-related subsystem
part of a E/E/PE safety-related system (for example a programmable controller) for which:
- the failure mode of at least one component is not well defined, or
- the behavior of the programmable controller under fault conditions cannot be completely determined, or
- there is insufficient field failure data to show that the claimed failure rates are met

logic element (logic system)
portion of a system that performs the logic function but excludes the sensors and the actuators (final elements)

mean time to restoration (MTTR)
time (measured in hours) from when a failure occurs to when functionality is restored

mode of operation
way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it, which may be either:
- low demand mode where the frequency of demands for operation made on a safety-related system is no greater than one to ten per year and no greater than the proof-test frequency
- high demand or continuous mode where the frequency of demands for operation made on a safety-related system is greater than ten per year or greater than twice the proof-test frequency

MooN
M out of N channel architecture.
NOTE 1: In a M out of N channel architecture, M out of N channels are required to function properly for the system to function properly.
NOTE 2: If there are N channels and M of those are required for the system to function properly, then the system can tolerate (N – M) failures.

Probability of Failure on Demand (PFD)
average probability to perform the design function on demand (applicable to a low demand mode of operation)

Probability of Failure per Hour (PFH)
probability of a dangerous failure per hour (applicable to a high demand or continuous mode of operation)

programmable electronic system (PES)
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (taken from IEC 61508-4)

proof test
periodic test performed to detect failures

risk
combination of the probability of occurrence of harm and the severity of that harm (taken from IEC 61508-4)

random hardware failure
failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware (taken from IEC 61508-4)

safe failure fraction
- the safe failure fraction of a subsystem is the ratio of the average rate of safe failures plus dangerous detected failures divided by the average failure rate of the subsystem

safety integrity
probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time (taken from IEC 61508-4)

safety integrity level (SIL)
discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest (taken from IEC 61508-4)
NOTE: this specification scheme is only applicable to the safety-related **system**

safety related system
designated system that both:
- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other E/E/PE safety-related systems, other safety technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions (taken from IEC 61508-4)

safety requirements specification (SRS)
specification containing all the requirements of the safety functions that have to be performed by the safety-related systems (taken from IEC 61508-4)

systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors (taken from IEC 61508-4)

verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled (taken from IEC 61508-4)

4 Conformance to this standard

Conformance to this standard is only required when a programmable controller is advertised and intended to be used with a safety-related system.

There are several steps in conforming to this standard. Since the related actions occur throughout the lifecycle of a programmable controller, they are addressed by the relevant lifecycle phases established in IEC 61508. Those applied in this standard are:

Characterization requirements
Functional validation planning
Design and development
Integration
Operation and maintenance
Functional validation
Modification
Verification

The requirements and outputs of these lifecycle phases are specified in clauses 5 through 12. Conformance to these clauses is the responsibility of the programmable controller manufacturer.

5 Characterization requirements

A Safety Requirements Specification (SRS) shall be generated during the functional safety requirements phase of the lifecycle of a programmable controller. It shall contain:

-a description of all programmable controller functions (potentially related to safety) including: design requirements, the manner in which a specific state is achieved and maintained, and whether high/continuous and/or low demand of operation is targeted

NOTE: A programmable controller is generally used in a low demand safety application.

- response time
- all external and human machine interfaces
- a description of all relevant modes of operation
- failures and faults taken into account and the corresponding responses
- constraints between hardware and software
- limiting constraints between the programmable controller and the safety-related system
- start-up and restarting requirements
- the PFD or PFH range for undetected potentially dangerous failures of the programmable controller

NOTE 1: This range (see the third column of Tables 1 and 2) is based on the targeted SIL for the safety-related system (see the first two columns of Tables 1 and 2) and the allocation of 10% of the system's PFD or PFH to the programmable controller
NOTE 2: The PFD of a safety-related system is the sum of the PFD values for the sensors, the logic element, and the actuators.

- environmental condition limits
- electromagnetic immunity limits

Table 1 - Safety Integrity Levels – for Low Demand Mode of Operation

SIL of safety-related system	Average Probability of Failure of the safety-related system to perform its design function on Demand (PFD)	Average Probability of Failure of the programmable controller to perform its design function on Demand (PFD)
4	$\geq 10^{-5}$ to 10^{-4}	$\geq 10^{-6}$ to 10^{-5}
3	$\geq 10^{-4}$ to 10^{-3}	$\geq 10^{-5}$ to 10^{-4}
2	$\geq 10^{-3}$ to 10^{-2}	$\geq 10^{-4}$ to 10^{-3}
1	$\geq 10^{-2}$ to 10^{-1}	$\geq 10^{-3}$ to 10^{-2}

Table 2 - Safety Integrity Levels - for High Demand or Continuous Mode of Operation

SIL of safety-related system	Probability of dangerous safety-related system Failures per Hour (PFH)	Probability of potentially dangerous programmable controller Failures per Hour (PFH)
4	$\geq 10^{-9}$ to 10^{-8}	$\geq 10^{-10}$ to 10^{-9}
3	$\geq 10^{-8}$ to 10^{-7}	$\geq 10^{-9}$ to 10^{-8}
2	$\geq 10^{-7}$ to 10^{-6}	$\geq 10^{-8}$ to 10^{-7}
1	$\geq 10^{-6}$ to 10^{-5}	$\geq 10^{-7}$ to 10^{-6}

6 Functional safety validation planning

This phase of the lifecycle of a programmable controller is usually carried out in parallel with its design and development. It is accomplished by specifying the steps that are to be used to demonstrate compliance to the SRS. The functional safety validation plan shall include the procedures to be followed, a description of the test environment, and pass/fail criteria.

7 Design and development

The design and development phase of the safety lifecycle is critical in assuring that the programmable controller meets the PFD or PFH criteria established in the SRS.

Since a programmable controller can generally be used for both safety and non-safety functions, all hardware and software shall be treated as safety-related unless safety and non-safety functions can be made independent. When this independence is part of the design, the method of achieving this independence and the justification of the method must be documented.

The following items are considered necessary to the overall evaluation of a programmable controller as a logic element of a safety-related system and must be documented during the design and development lifecycle phase:

a) a specification of those functions and interfaces which can be used by safety functions
b) estimates of random hardware failure rates which could cause a dangerous system failure and which are detected by diagnostic tests
c) estimates of random hardware failure rates which could cause a dangerous system failure and which are **not** detected by diagnostic tests
d) environmental limits to maintain failure rate validity
e) any limits on the useful lifetime which should not be exceeded to maintain the validity of the failure rate estimates
f) periodic proof test and/or maintenance requirements
g) diagnostic coverage internal to the programmable controller
h) diagnostic test interval internal to the programmable controller
i) Mean Time To Restoration (MTTR)
j) Safe Failure Fraction (SFF)
k) hardware fault tolerance
l) application limits recommended to avoid systematic failures
m) SILs that can be claimed for the safety-related systems that the programmable controller will be fit for use with
n) hardware and software configuration of the programmable controller
o) documentary evidence that a subsystem has been validated (see clause 10)

7.1 Random Hardware Failures

Random hardware failure rates can be determined by failure modes and effects analysis (FMEA) of the design using component failure data from a recognized industry source, or from experience of the previous use of the programmable controller in a similar environment. Failure rate data should have a confidence level of at least 70% as defined in IEEE 352 (or an equivalent "significance level" per IEC 61164). "Proven in use" data shall be based on operational time of at least one year and shall be sufficient to establish a confidence limit of at least 70%. Only previous operation where all failures have been detected and reported and where conditions of use are similar shall be considered.

Once these failure rates are determined, the architecture of the "logic element" of the safety-related system must be established. This is a prerequisite to determining the PFD or PFH value of the logic element. The following clauses address the PFD and PFH calculations for 1oo1, 1oo2, 1oo2D (with diagnostics), 2oo2, and 2oo3 architectures of a programmable controller.

7.1.1 1oo1 architecture

A 1oo1 architecture is the simplest to consider. Only one channel or logic path is present. A dangerous fault or failure in this path leads to a dangerous failure of the safety function when a demand arises.

For a programmable controller with a 1oo1 architecture used in a low demand mode of operation, the average Probability of Failure on Demand is:

$$\mathbf{PFD} = [\lambda_{DU} + \lambda_{DD}]\, t_{CE}$$

where:

λ_{DU} = the undetected dangerous failure rate per hour
λ_{DD} = the detected dangerous failure rate per hour
t_{CE} = the mean channel downtime (in hours).

For a programmable controller with a 1oo1 architecture used in a high demand or continuous mode of operation, the average Probability of Failure per Hour is:

$$\mathbf{PFH = \lambda_{DU}}$$

Where it is assumed that the safety system puts the EUC into a safe state on the detection of any failure.

7.1.2 1oo2 architecture

In a 1oo2 architecture, either channel can process the safety function. There would have to be a dangerous failure in both channels before a safety function failed.

For a low demand mode of operation, the average Probability of Failure on Demand for a programmable controller with a 1oo2 architecture is:

$$\mathbf{PFD = 2[(1 - \beta_D)\,\lambda_{DD} + (1 - \beta)\,\lambda_{DU}]^2\, t_{CE}\, t_{GE} + \beta_D\,\lambda_{DD}\,MTTR + \beta\lambda_{DU}\,[(T_1/2) + MTTR]}$$

where:

β_D = the fraction of detected failures having a common cause,
t_{GE} = the mean downtime for both channels (in hours)
MTTR = the mean time to restoration (in hours)
T_1 = the proof test interval (in hours)

NOTE: The proof test interval is typically specified for a low demand mode of operation as 6 months (4380 hours) or 1 year (8760 hours).

For a programmable controller with a 1oo2 architecture used in a high demand or continuous mode of operation, the Probability of Failure per Hour is:

$$\mathbf{PFH = 2[(1 - \beta_D)\,\lambda_{DD} + (1 - \beta)\,\lambda_{DU}\,]^2\, t_{CE} + \beta_D\,\lambda_{DD} + \beta\,\lambda_{DU}}$$

7.1.3 1oo2D architecture

In this architecture, both channels must demand the same safety function before it can take place. If diagnostics detect a fault in one channel, the output state follows that given by the other channel. If both channels fault or a discrepancy cannot be allocated to either channel, the output goes to a safe state.

The average Probability of Failure on Demand for a programmable controller with a 1oo2D architecture is:

$$\mathbf{PFD = 2(1 - \beta)\,\lambda_{DU}\,[(1 - \beta)\,\lambda_{DU} + (1 - \beta_D)\,\lambda_{DD} + \lambda_{SD}]\, t_{CE}\, t_{GE} + \beta_D\,\lambda_{DD}\,MTTR + \beta\,\lambda_{DU}\,[(T_1/2) + MTTR]}$$

where:

β = the fraction of undetected failures that have a common cause.

For a programmable controller with a 1oo2D architecture used in a high demand or continuous mode of operation, the Probability of Failure per Hour is:

$$PFH = 2\,(1 - \beta)\,\lambda_{DU}\,[(1 - \beta)\,\lambda_{DU} + (1 - \beta_D)\,\lambda_{DD} + \lambda_{SD}]\;\; t_{CE}' + \beta_D\,\lambda_{DD} + \beta\,\lambda_{DU}$$

where:

$\lambda_{SD} = \lambda_D$ DC

t_{CE}' = the channel equivalent mean downtime (in hours)

7.1.4 2oo2 architecture

In this architecture, both channels must demand the safety function before it can take place.

The average Probability of Failure on Demand of a programmable controller with a 2oo2 architecture is:

$$PFD = 2\,(\lambda_{DU} + \lambda_{DD})\,t_{CE}$$

For a high demand or continuous mode of operation, the Probability of Failure per Hour of a programmable controller with a 2oo2 architecture is:

$$PFH = 2\,\lambda_{DU}$$

7.1.5 2oo3 architecture

This architecture consists of three channels connected in parallel with a majority voting arrangement for the output signals.

In a low demand mode of operation, the average Probability of Failure on Demand for a programmable controller with a 2oo3 architecture is:

$$PFD = 6\,[(1 - \beta_D)\,\lambda_{DD} + (1 - \beta)\,\lambda_{DU}]^2\,t_{CE}\,t_{GE} + \beta_D\,\lambda_{DD}\,MTTR + \beta\,\lambda_{DU}\,[(T_1/2) + MTTR]$$

In a high demand or continuous mode of operation, the Probability of Failure per Hour for a programmable controller with a 2oo3 architecture is:

$$PFH = 6\,[(1 - \delta_D)\,\lambda_{DD} + (1 - \beta)\,\lambda_{DU}]^2\,t_{CE} + \beta_D\,\lambda_{DD} + \beta\,\lambda_{DU}$$

7.2 Software Considerations

When a programmable controller is to be used in a safety application, the software design and development activities shall comply with the requirements of this clause.

(Author's note: This clause will be added at a later date)

7.3 Systematic Failures

Systematic failures are failures that are related to a cause which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. Since systematic failures generally only contribute a few percent to the overall failure rates of programmable controllers, their consideration is omitted in the standard.

7.4 Diagnostic Coverage

The diagnostic coverage of a programmable controller can be calculated as follows:

a) carry out a Failure Mode and Effects Analysis (FMEA) of each failure mode of each component
b) categorize each failure mode according to whether it leads to a safe failure (or safe shut-down)or a dangerous failure

NOTE: A programmable controller is considered a high complexity safety-related subsystem where it can be assumed that 50% of the random hardware failures are safe and 50% are dangerous.

c) calculate the probability of safe failures (λ_S) and the probability of dangerous failures (λ_D)
d) estimate the probability of dangerous failures which will be detected by diagnostic tests (λ_{DD})
e) calculate the probability of dangerous failures which will not be detected by diagnostic tests (λ_{DU})

NOTE: $\lambda_D = \lambda_{DD} + \lambda_{DU}$

f) Calculate the diagnostic coverage (DC):

$$\mathbf{DC = \Sigma \lambda_{DD} / \Sigma \lambda_D = \Sigma \lambda_{DD} / [\Sigma \lambda_{DU} + \Sigma \lambda_{DD}]}$$

Table 3 lists the faults or failures that shall, as a minimum, be detected in order to achieve a 90 to 99% diagnostic coverage for a single fault tolerant programmable controller fit for use in a SIL 1, 2, or 3 safety-related system. IEC 61508 should be referred to for other situations.

Table 3 - Faults or failures to be detected and controlled to achieve a 90 to 99% diagnostic coverage in a single fault tolerant programmable controller fit for use in a SIL 1, 2, or 3 safety-related system

COMPONENT	FAULT OR FAILURE	EXAMPLES OF POSSIBLE DIAGNOSTIC MEASURES
Electromechanical Devices	Devices energize or de-energize unintentionally Individual contacts weld	Contact monitor Majority voting Comparator
Digital I/O	A signal line is permanently high or permanently low Adjacent signal lines are shorted Timing failures Addressing failures	Test Pattern Multi-channel parallel outputs Monitored outputs Input comparison/voting Superimposing a carrier frequency signal
Analog I/O	A signal line is permanently high or permanently low Drift and oscillation occur	Test pattern Multi-channel parallel outputs Monitored outputs

	Timing failures Addressing failures	Input comparison/voting
Power Supply	Shorts between two leads Drift and oscillation	Over/under voltage detection with safe power down or switchover to back-up Secondary voltage monitor with safe power down or switchover to back-up
Bus		
- general	Time out	Input comparison/voting
- memory management unit	Wrong address decoding	Multi-bit hardware redundancy Complete hardware redundancy
- direct memory access	Data/addresses do not change Wrong access time	Inspection using test patterns Transmission redundancy
- bus arbitration	No, constant, or wrong arbitration Cross-talk	Information redundancy
CPU		
- coding, execution	Wrong coding or wrong execution	Majority voting Comparator
- address calculation	Addresses do not change Signal lines/gates short	Reciprocal comparison by software
- register, internal RAM	Data/addresses do not change Signal lines/gates short	Coded processing Walking-bit
- program counter, stack pointer	Data does not change Signal lines/gates short	Watchdog with separate time base & time window Temporal & logical monitoring of program sequence
Interrupt Handling	No or continuous interrupts, crossover of interrupts	Comparator Majority voting
Invariable Memory (e.g. ROM, EEPROM)	Data/addresses do not change Signal lines/gates short	Signature of a double word Block replication Hamming code Modified checksum
Variable Memory (e.g. RAM, FLASH)	Data/addresses do not change Signal lines/gates short Cross-talk Dynamic failures/coupling Odd bit/two bit failures	RAM test - galloping pattern RAM test - walk path RAM monitoring with modified Hamming code Data failure detection with error-detection-correction codes
Clock (quartz)	Sub- or super-harmonics Defective program sequence	Watchdog with separate time base & time window Temporal & logical monitoring
Communication & Mass Storage	Wrong data or addresses Cross-talk	Separation of electrical energy lines from information lines Separation of multiple information lines Increase interference immunity
Task Scheduling		
Memory Management Software		

Data Communication
Software

Application Software

User Interface
Software

7.5 Safe Failure Fraction

The safe failure fraction is defined as the total safe failure rate divided by the total failure rate. In terms of the parameters defined above it can be expressed as:

$$\mathbf{SFF = (\Sigma \lambda_S + \Sigma \lambda_{DD}) / (\Sigma \lambda_S + \Sigma \lambda_D)}$$

For complex subsystems like programmable controllers, a division of failures into 50% safe and 50% dangerous is generally accepted.

The detection of a dangerous fault in a programmable controller with a hardware fault tolerance of 1 or more shall result in either a specified action: to achieve or maintain a safe state (or shutdown) or, to isolate the faulty part to allow continued safe operation.

The detection of a dangerous fault in a programmable controller having a hardware fault tolerance of zero shall result in either a specified action: to achieve or maintain a safe state (or shutdown) or, the repair of the faulty programmable controller within the mean time to restoration (MTTR).

7.6 Random Hardware Fault Tolerance

Also during design of the programmable controller, its random hardware fault tolerance shall be defined. A hardware fault tolerance of N means that N + 1 faults could cause a loss of a safety function. The fault tolerance needed for the programmable controller is a function of the targeted SIL of the safety-related system and the safe failure fraction of the programmable controller. Table 4 shows this relationship.

Table 4 – Hardware safety integrity – high complexity systems

SFF	Hardware Fault Tolerance		
	0	1	2
< 60%	Not Allowed	SIL 1	SIL 2
60% to < 90%	SIL 1	SIL 2	SIL 3
90% to < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

7.7 Common Cause Failures

A common cause failure is a failure which is the result of one or more events and which causes coincident failures of two or more separate channels in a multiple channel system. These

failures are included in the equations of clause 7.1 through "β" factors. Specific values for β and β_D are obtained from Table 5 where S and S_D are calculated from the following equations:

$$\mathbf{S = X + Y}$$

$$\mathbf{S_D = X [Z + 1] + Y}$$

The values of X, Y, and Z are the sums of the values of X_{LS} and Y_{LS} obtained from tables D.1 of IEC 60508-6 for a logic subsystem; and Z is obtained from Table 6 (assuming a diagnostic test interval of less than one minute).

Table 5 – Values of β and β_D

S or S_D	Values of β or β_D
120 and above	0.5%
70 to 120	1%
45 to 70	2%
Less than 45	5%

Table 6 – Values of Z for programmable electronics

Diagnostic Coverage	Values of Z
≥ 99%	2.0
≥ 90%	1.5
≥ 60%	1.0

7.8 Data Communications

When any form of data communication is used in the implementation of a safety function, the probability of undetected failure of the communication process shall be estimated taking into account transmission errors, repetitions, deletions, insertion, resequencing, corruption, delay, masquerade. The following parameters shall be taken into account when estimating the probability of failure of the safety function due to the communications process:

- The residual error rate
- the rate of residual information loss,
- the limits and variability of the rate of information transfer,
- the limits and variability of the information propagation delay time

NOTE: The probability of a dangerous failure per hour associated with data communications is the quotient of the residual error probability and the message length (in bits) multiplied by the bus transmission rate and the factor 3600.

8 Integration

The integration phase of the safety lifecycle of a programmable controller consists primarily of functional testing, and either black-box or statistical testing or field experience. These tests shall show that all modules, and sub-parts thereof, interact correctly to perform their intended function.

9 Operation and maintenance

To satisfy the operation and maintenance phase of the safety lifecycle of a programmable controller, operation and maintenance procedures shall be prepared and shall state:

a) routine actions needed to maintain "as-designed" functional safety
b) actions and constraints needed during installation, start-up, shut-down, etc to prevent an unsafe state
c) procedures to be followed when faults or failures occur

For a SIL 3 system, the following measures are recommended to avoid faults and failures:

a) adequate and understandable instructions
b) user friendliness
c) minimum and simple maintenance
d) limited operation possibilities
e) protection against operator mistakes
f) operation by skilled and trained operators only

NOTE: Operating and maintenance procedures shall include software modification procedures.

10 Safety validation

Validation is a confirmation – with supportive evidence – that a desired result occurs and that a particular requirement is fulfilled. The validation process shall be carried out according to the safety validation plan created during the design and development phase.

Each safety function specified in the SRS shall be validated by test and/or analysis under various environmental conditions. Surge immunity testing according to IEC 61000-4-5 shall be performed. For a diagnostic coverage ≥ 90% fault insertion testing shall be performed. Also, either static/dynamic/failure analysis, or simulation and failure analysis, or worst case analysis must be performed. Lastly either fault insertion, statistical, or worst case testing, or field experience must be documented (for a SIL 3 system).

The outcome of the validation phase shall include: specific references to the validation plan, specific requirements of the programmable controller, equipment used during the validation, equipment calibration data, and results for each test.

A validation report shall be made available to a developer of a safety-related system.

11 Modification

Manufacturers that claim compliance with this standard shall maintain a system to initiate changes as a result of the detection of defects. This system shall include the documentation of: details of the modification, analyses of its impact, approvals for the modification, revalidation results, and any associated changes to a product's operation or documentation. This system shall also inform users of the need for modification if the defect affects safety.

After modification, the programmable controller shall also be reverified.

12 Verification

This phase of the lifecycle is actually performed during several other phases of the lifecycle. For example, during design and development, outputs must be tested to ensure their correctness and consistency with inputs, and it must be demonstrated that the specific faults and failures given in

Table 3 are detected.